

Phát hiện chiến dịch tấn công có chủ đích APT quy mô lớn vào các tổ chức trọng yếu tại Việt Nam

16:42 01/10/2022

Công ty Công nghệ an ninh mạng Việt Nam NCS vừa phát hiện một chiến dịch tấn công có chủ đích APT quy mô lớn vào các công ty, tổ chức, trọng yếu tại Việt Nam.



Ảnh minh họa. (Ảnh: internet)

Chiến dịch tấn công này khai thác vào lỗ hổng Zero-day của Microsoft Exchange, một trong những phần mềm mail server phổ biến nhất trong các cơ quan, tổ chức tại Việt Nam.

Nhận định lỗ hổng mới rất nghiêm trọng, ảnh hưởng tới nhiều đơn vị trọng yếu tại Việt Nam, các chuyên gia NCS đã ngay lập tức nghiên cứu và phát hiện ra

mã khai thác exploit, sau đó, thông tin tới tổ chức ZDI làm việc với Microsoft, để hãng có thể cập nhật nhanh chóng bản vá.

Cùng với việc cảnh báo về chiến dịch tấn công APT quy mô lớn nhằm vào các tổ chức, doanh nghiệp trọng yếu tại Việt Nam qua khai thác lỗ hổng trên máy chủ Microsoft Exchange, Công ty NCS cũng phát hành công cụ miễn phí kiểm tra.

NCS đã phát hành công cụ miễn phí NCS E0 Scanner, hỗ trợ các quản trị hệ thống quét máy chủ Microsoft Exchange để kiểm tra đã bị tấn công hay chưa. Để kiểm tra, nhân viên quản trị hệ thống tải công cụ kiểm tra NCS E0 Scanner tại địa chỉ github.com/ncsgroupvn/NCSE0Scanner, chạy trên máy chủ và bấm nút quét, công cụ sẽ thông báo cho người kiểm tra chi tiết các nhật ký ghi thông tin hệ thống nếu phát hiện ra máy chủ đã bị tấn công.

Ngoài ra, NCS cũng đã công bố mã nguồn của công cụ để hỗ trợ các quản trị có thể tự chỉnh sửa và xây dựng lại theo nhu cầu. Thông tin chi tiết về lỗ hổng zero-day của Microsoft Exchange do NCS nghiên cứu có thể xem trên các trang gteltsc.vn, bleepingcomputer.com hay success.trendmicro.com.

Trong thời gian chờ đợi Microsoft phát hành bản vá lỗi chính thức, các quản trị hệ thống sử dụng máy chủ Microsoft Exchange được khuyến cáo cần nhanh chóng rà soát toàn bộ hệ thống để phát hiện các dấu hiệu bất thường.

Hà Trần